ATM Cyber Security Awareness Workshop
Part II

ICAO AVSEC 2019

Montreal, Canada

Dr John HIRD

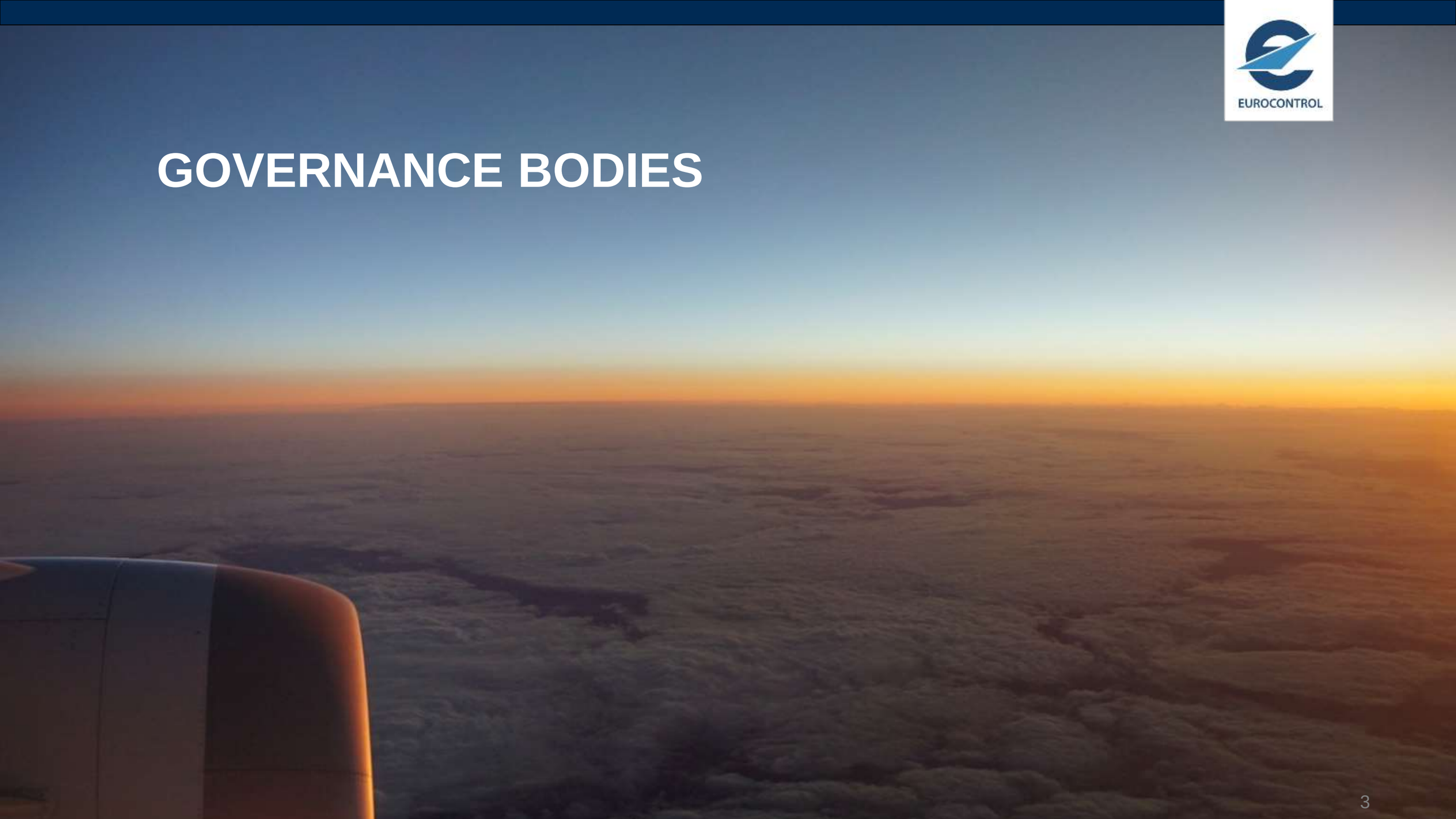
Air Traffic Management Security Specialist, EUROCONTROL

20th September 2019

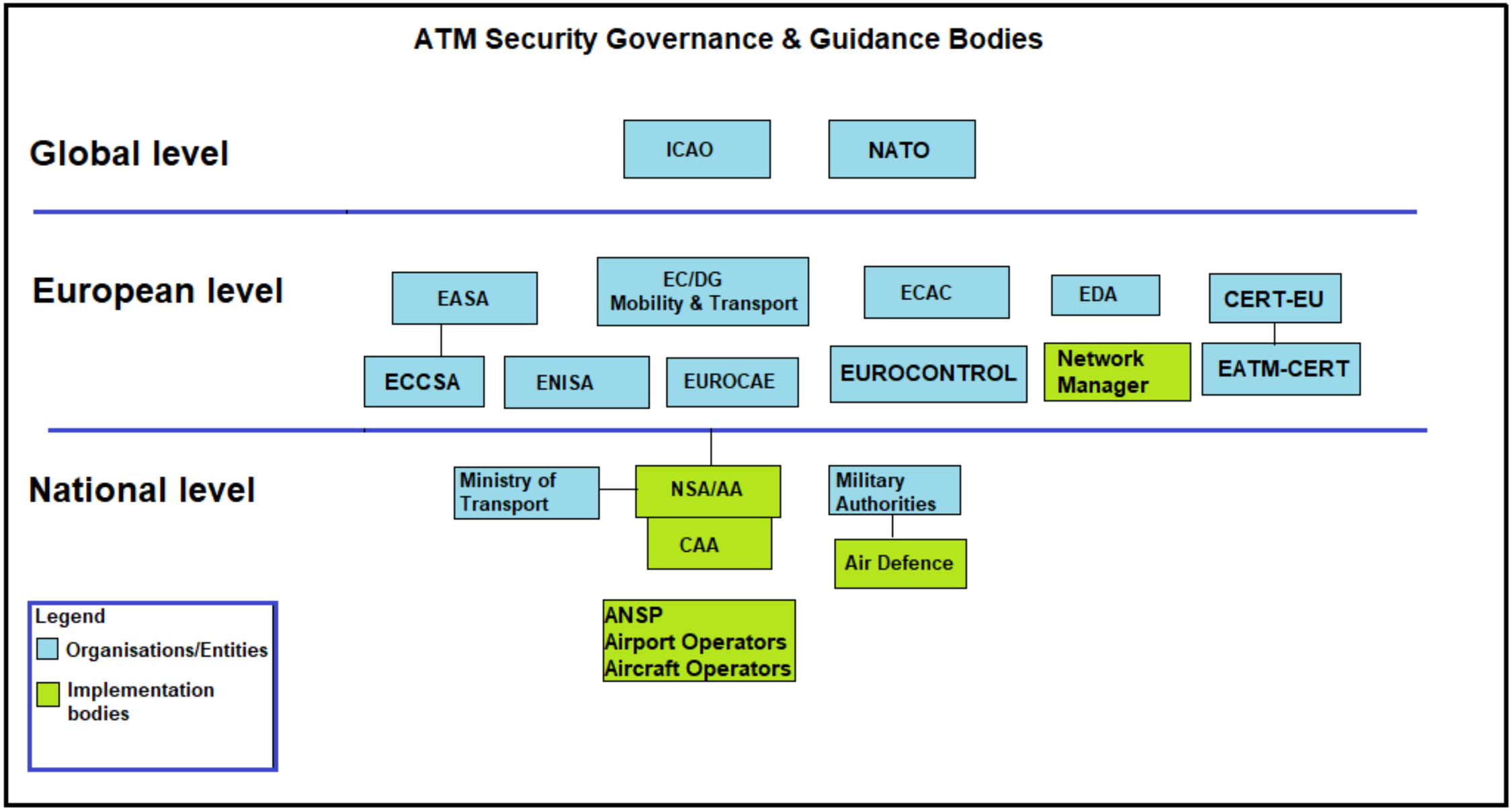
ATM Cybersecurity Awareness Workshop

	Part II – Responding to the Challenge
5	Governance Bodies
6	Regulations, Standards, and Guidance Material
7	Risk Management
8	Security Oversight
9	The Road Ahead
10	Trends in ATM Security
11	EUROCONTROL and the GASeP

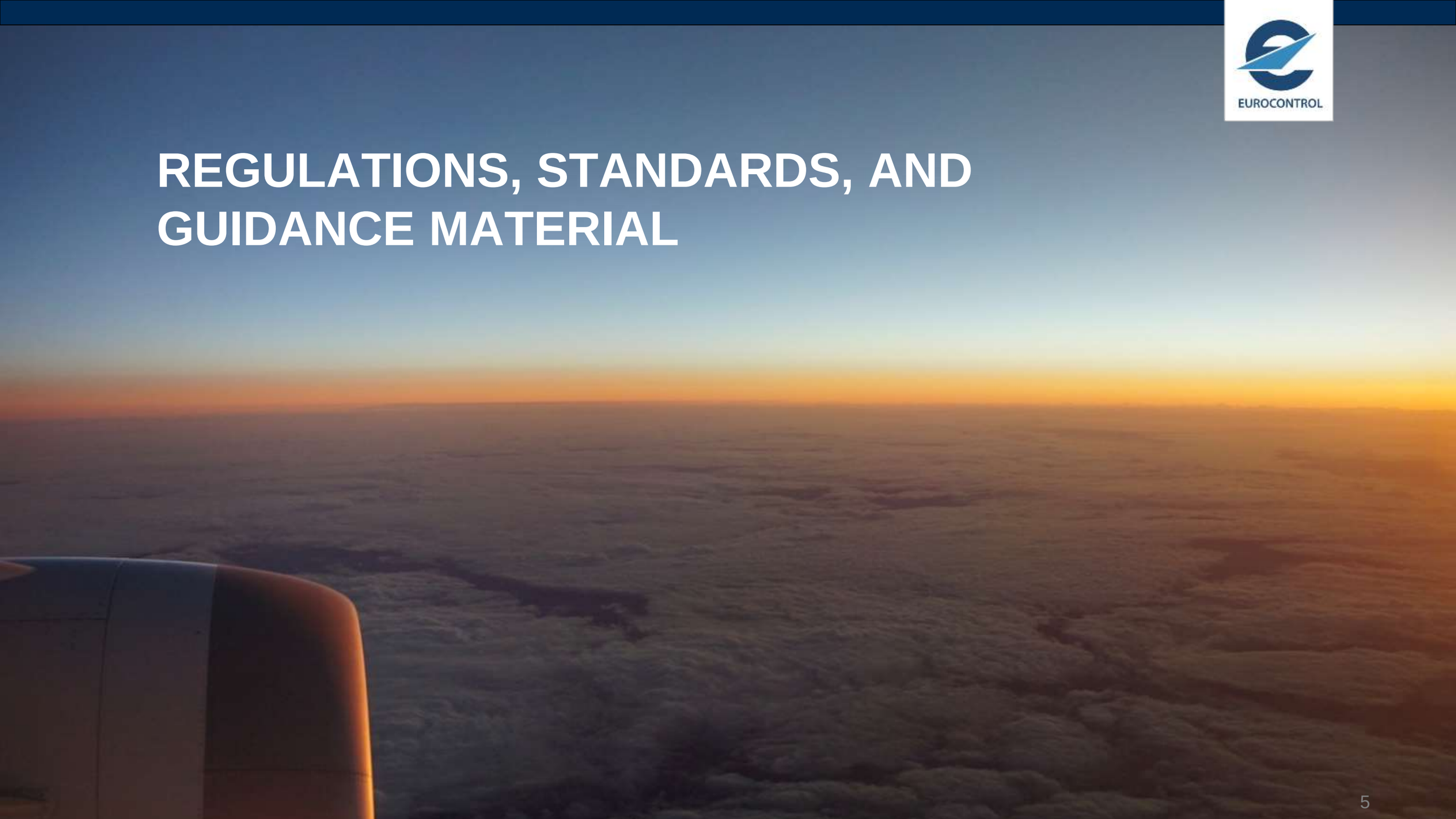
GOVERNANCE BODIES



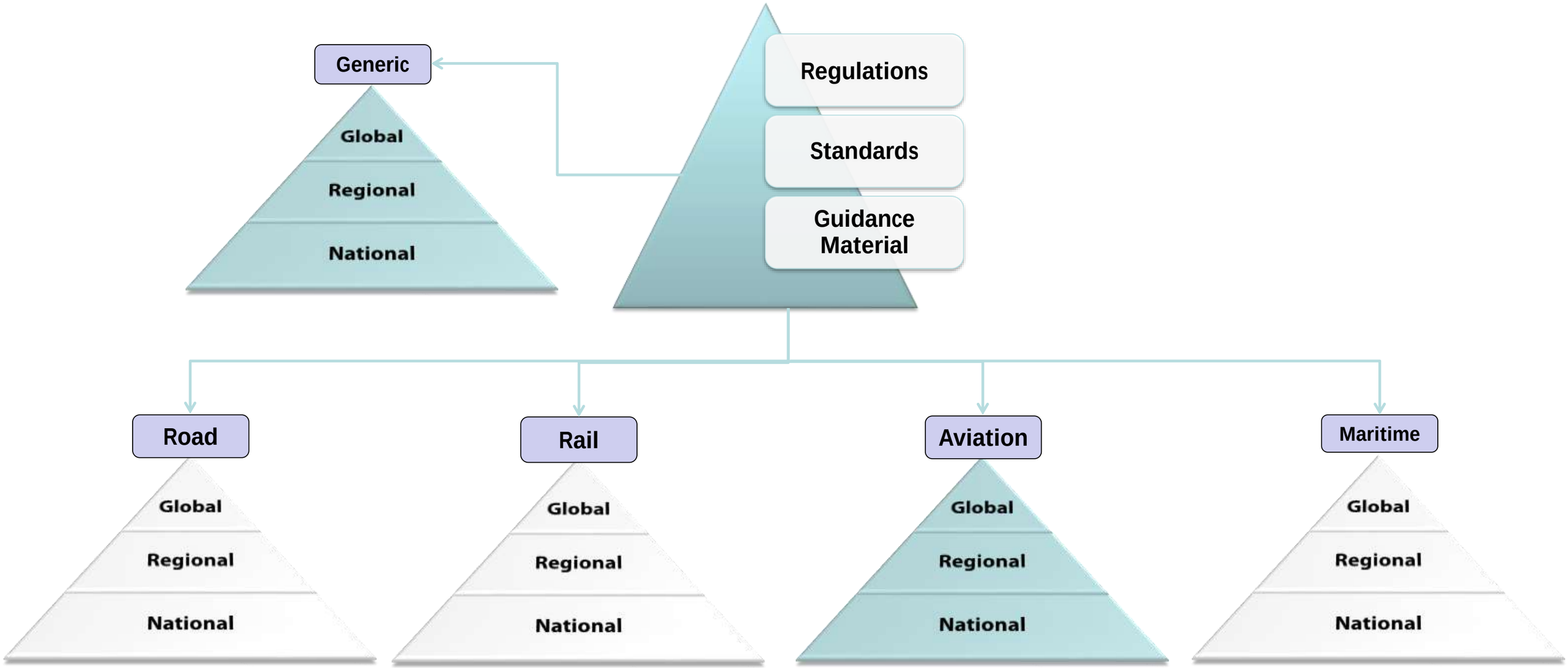
Governance Bodies



REGULATIONS, STANDARDS, AND GUIDANCE MATERIAL

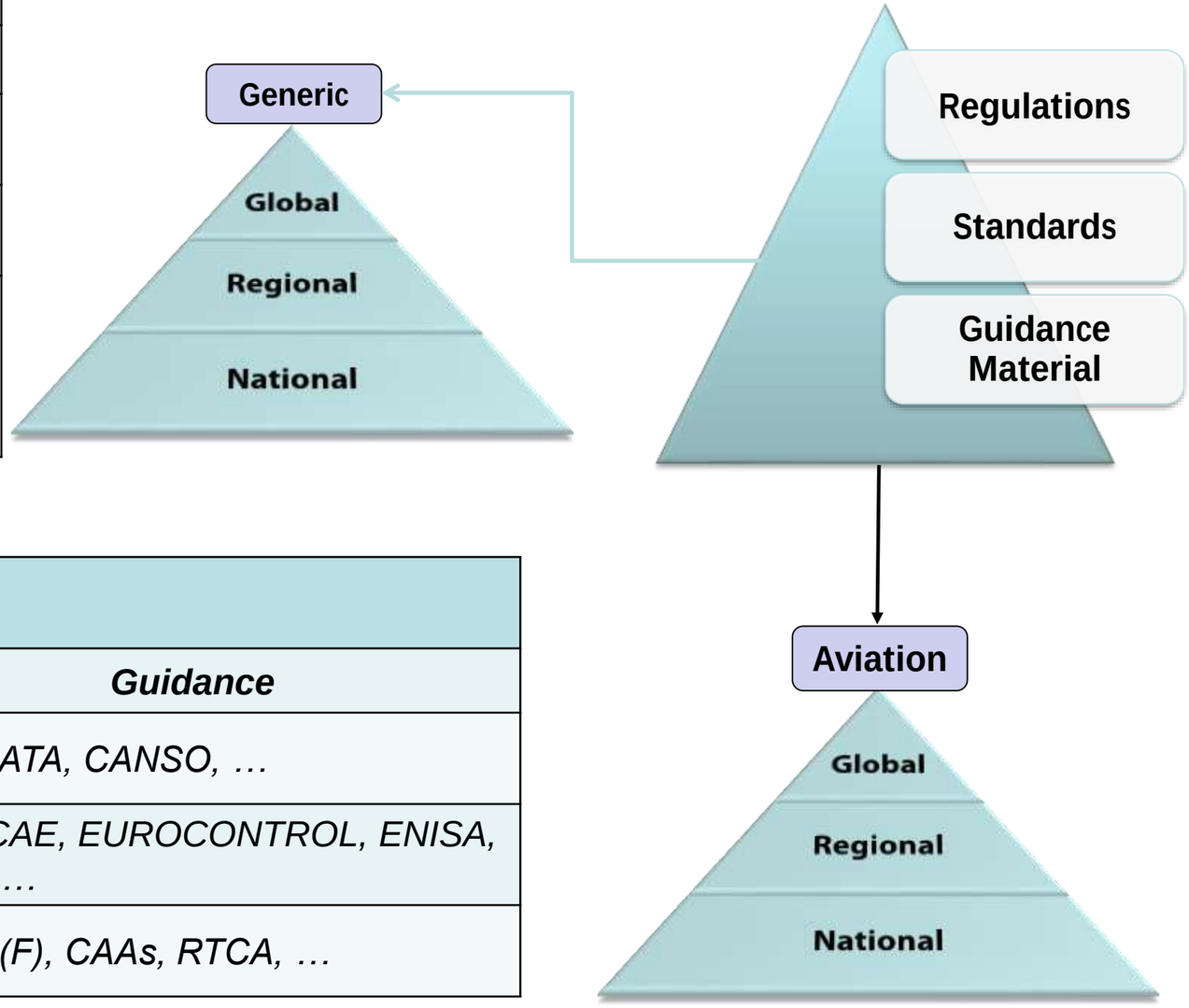


Regulations, Standards & Guidance Material



Regulations, Standards & Guidance Material

GENERIC			
	Regulations	***Standards***	***Guidance***
Global		*ISO, IEC, …*	
Regional			
National	*Government*	*ANSSI (F), BSI (D), NIST (US), NCCIC (US), …*	*ANSSI (F), BSI (D), NIST (US), NCCIC (US), SANS (US), …*



AVIATION			
	Regulations	***Standards***	***Guidance***
Global	*ICAO*	*ICAO*	*ICAO, IATA, CANSO, …*
Regional	*European Commission, EASA,*	*CEN*	*EUROCAE, EUROCONTROL, ENISA, ECAC, …*
National	*Government*		*ANSSI (F), CAAs, RTCA, …*

Aviation Security Regulations & Guidance - ICAO

Doc 8973 AVSec Manual

Doc 9854 ATM Op Concept, 2005

Annex 17 amend. 12, 2011 (ATSP, cyber)

Annex 17 amend. 13, 2013

Doc 9985 ATM Sec, 2013 (Secure design)

Annex 17 amend. 14, 2014

Doc 8973 AVSec, Ed.9, 2014

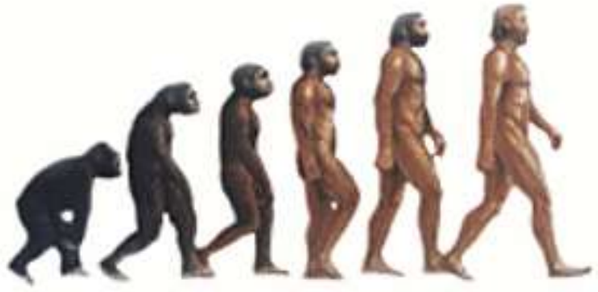
Doc 8973 AVSec, Ed.10, 2017

Annex 17 amend. 16, 2018

Doc 10047 AVSec Oversight Manual Ed.1, 2015

Doc 10108 Global Risk Context Statement Ed.1, 2018

2001 2005 2010 2016



Annex 17 - Security

- Aviation Security is a national responsibility, requiring international cooperation
- Amendment 12 – includes ANSPs, cybersecurity and supply-chain security within its scope
- Amendment 16 – includes provisions on information sharing and cyber threats

State

- make policy
- issue and enforce regulations
- inspect and monitor compliance

Airline

- screen passengers and baggage
- secure baggage and cargo
- protect aircraft
- security plan

Airport

- protect airside
- provide law enforcement support
- disposal of explosives
- security plan

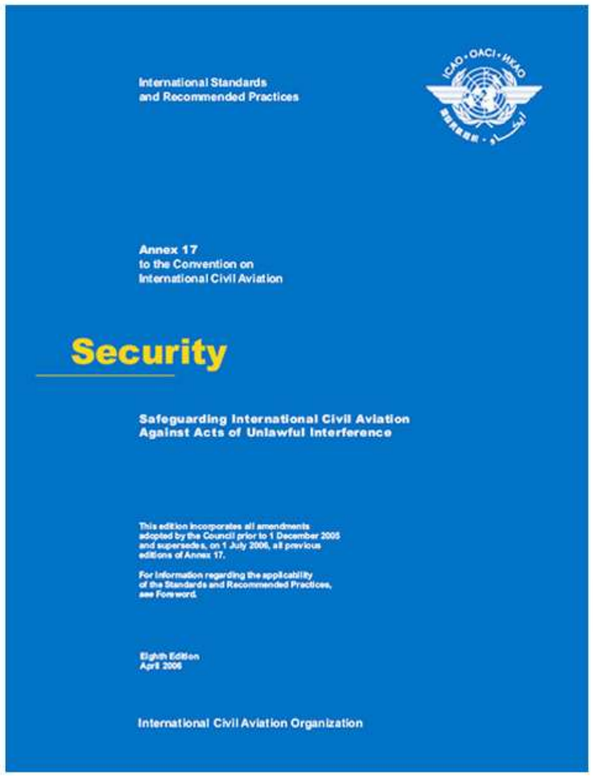
ATSP

Since Amendment 12, 2011

- Adequate security provisions
- Participate in national sec coordination

ICAO Annex 17 Guidance Material

Annex 17

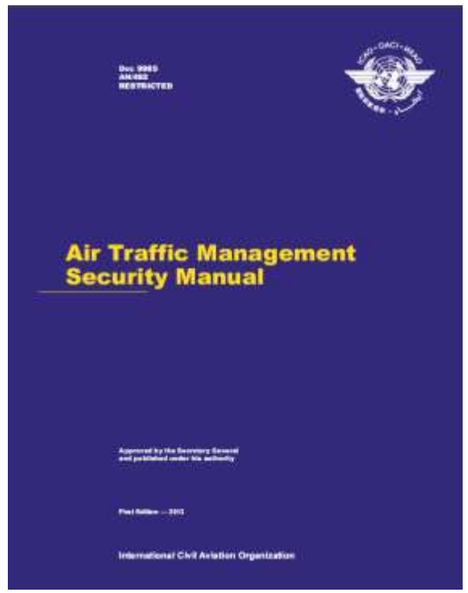


Security Manual

Doc 8973

** 8th edition – added Chapter 18 on cybersecurity

How to implement?

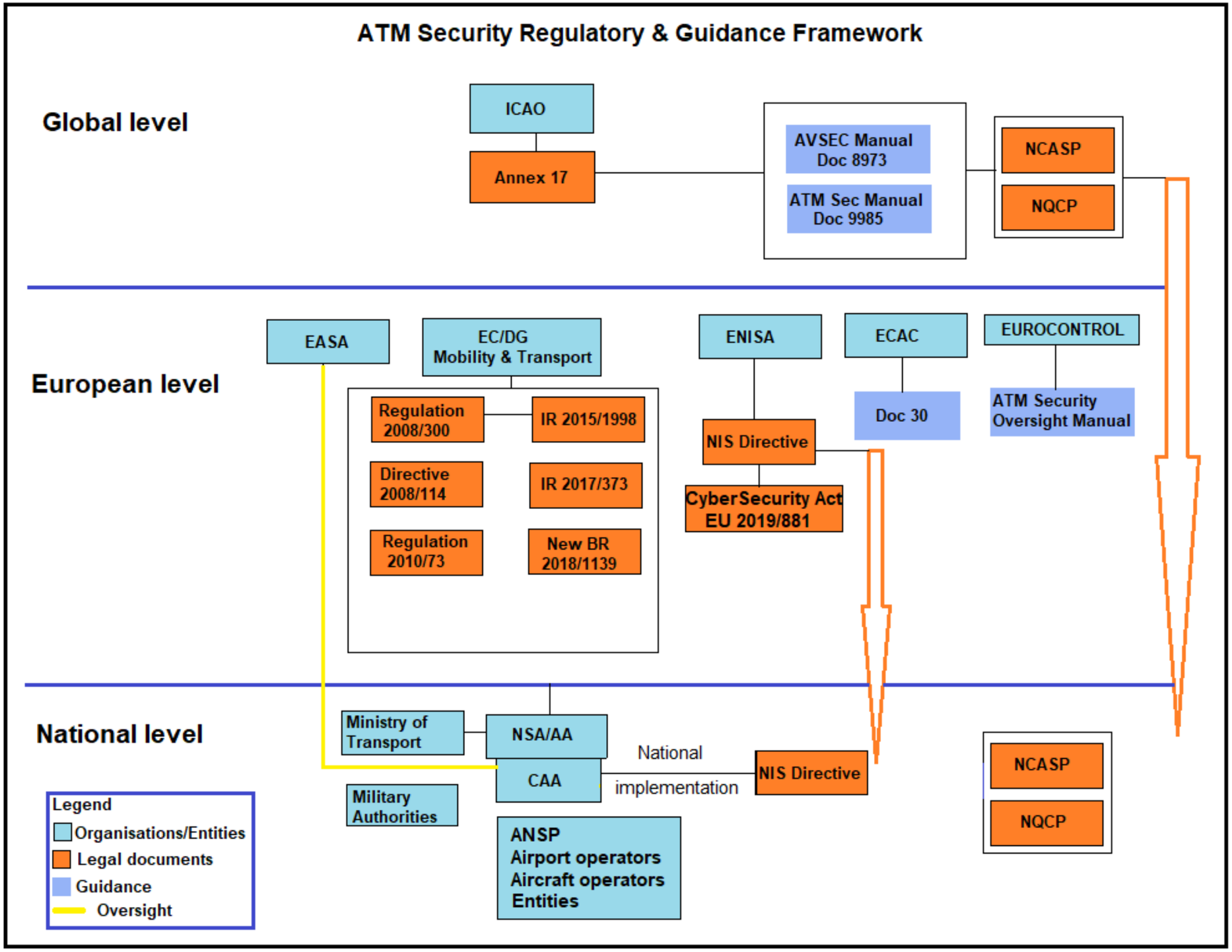


Doc 9985

ATM Security Manual

The Regulatory Framework

From a European region perspective

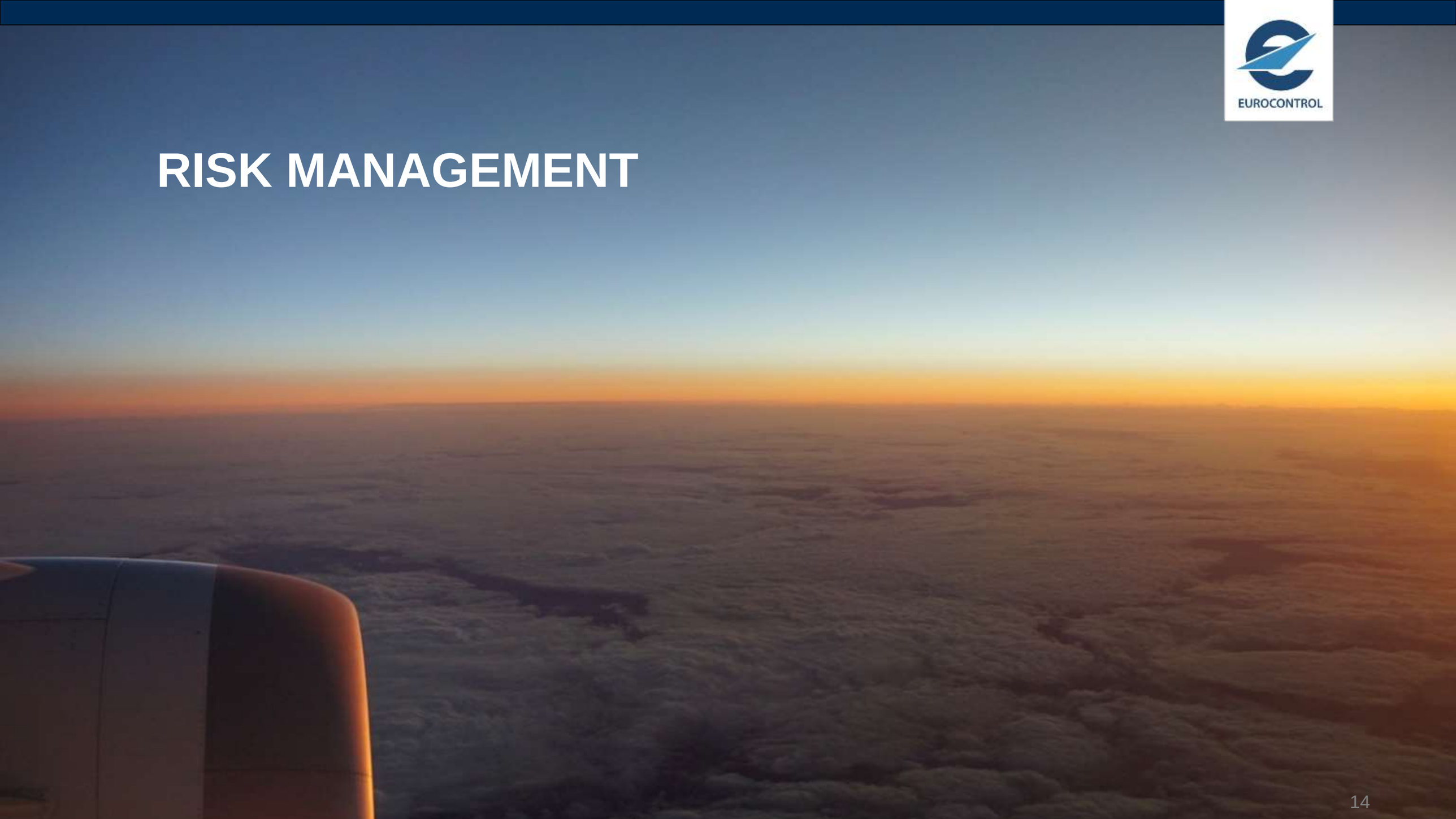


MENTI QUIZ : REGULATIONS, STANDARDS, …

- **Q7 : When did Annex 17 include ANSPs (ATSPs) and cybersecurity within its scope?**

- **Q8 : Doc 9985 contains …**

RISK MANAGEMENT



Security and Safety

We call **SAFETY** everything related to accidental events able to affect material and people (*failures,* …).

SECURITY concerns the prevention of deliberate malicious acts aimed at impacting the ATM system as a whole (theft, *hacking, jamming, spoofing, IED,* …).

Whatever can happen *accidentally* can be caused *deliberately*…

… the potential *impact* may be the same

Security versus Safety

Conflicting Requirements

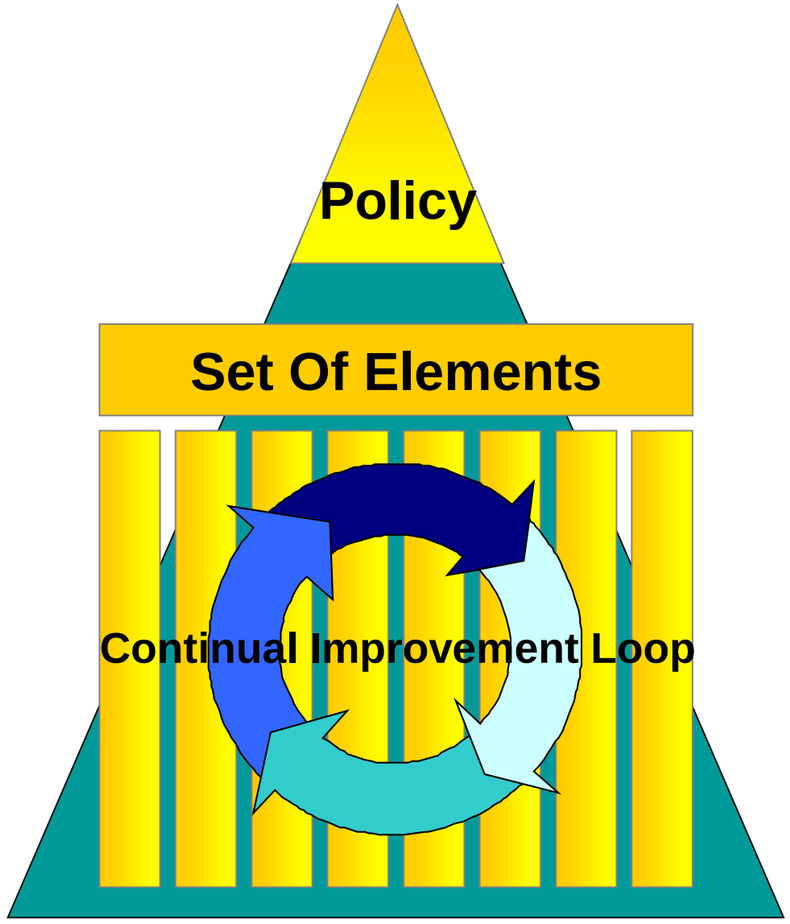
SAFETY
Concerned with human **error**, system **failure**, acts of god
Ease of access to users
Real-time system
Don't change the system
Test changes exhaustively

SECURITY
Concerned with **intentional** acts of **unlawful** interference
Restrict access
Controls may **impact performance**
Apply security **patches**
Update system quickly

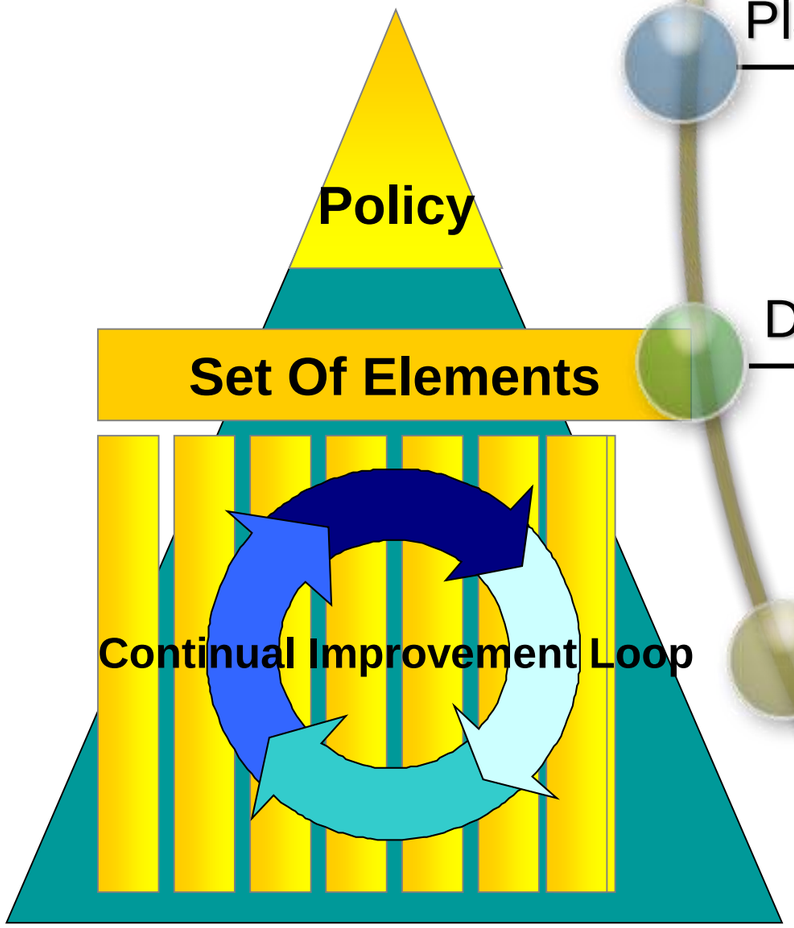
Security Management System (SeMS)

- What is a management system?

- **Aims and Expectations**
- **Processes**
- **Performance Standards (WHO/WHAT/WHEN)**
- **Management Procedures**
- **Operating Procedures & Practices**
- **Monitoring**



SeMS - Building Block Details



Plan

- Senior management commitment through Policy
- Security objectives, targets, programmes and initiatives that are consistent with the security policy
- The organizational structure, roles and responsibilities, human and financial resources, equipment and infrastructure
- The approach to risk-based management

Do

- Routine and security-related communications
- Operational control
- Information management

Check

- Compliance with legal, regulatory and other provisions
- Investigations of security-related failures, incidents non-conformance
- Performance measurement and analysis

Act

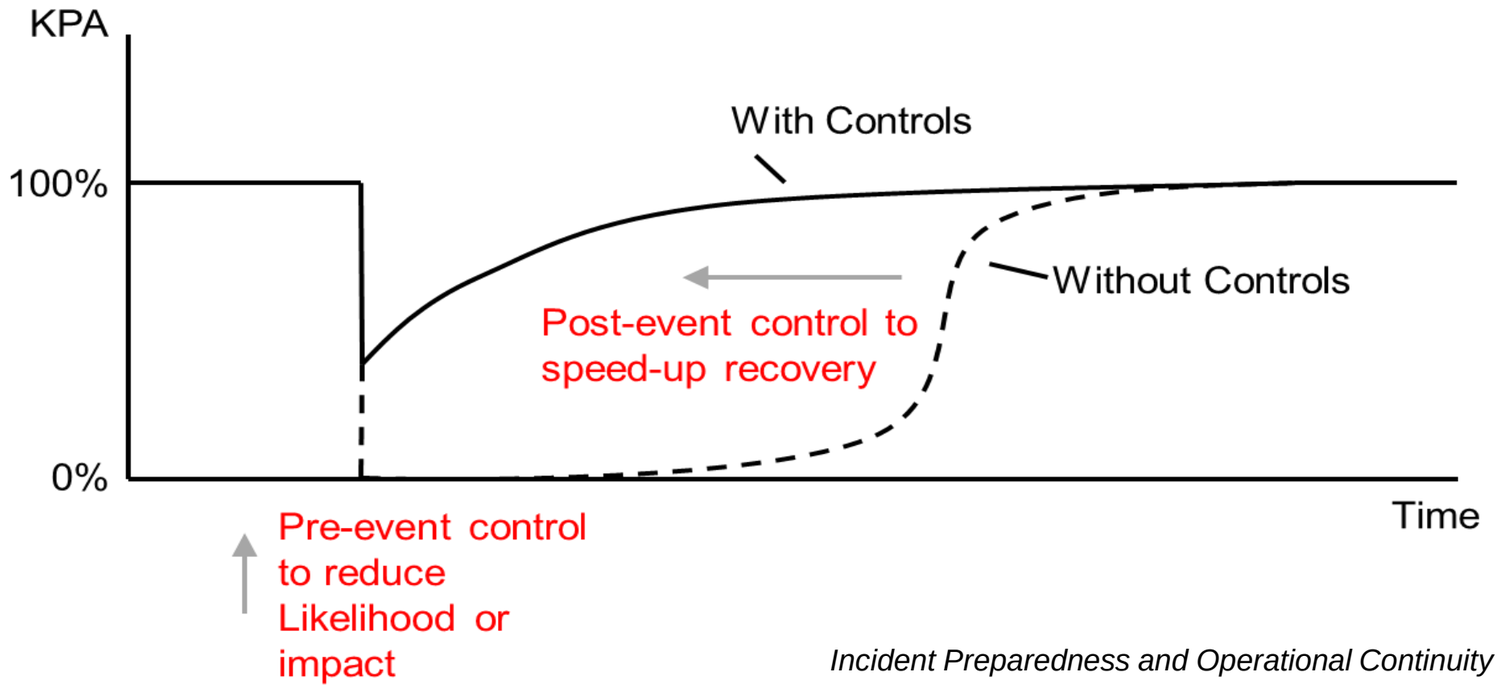
- Management of change and continual improvement.
- Periodic review of the SeMS
- Trend analysis and
- New technology assessment.

The ICAO SeMS

(See also Ch9 of Doc 8973)

(Cyber)Resilience

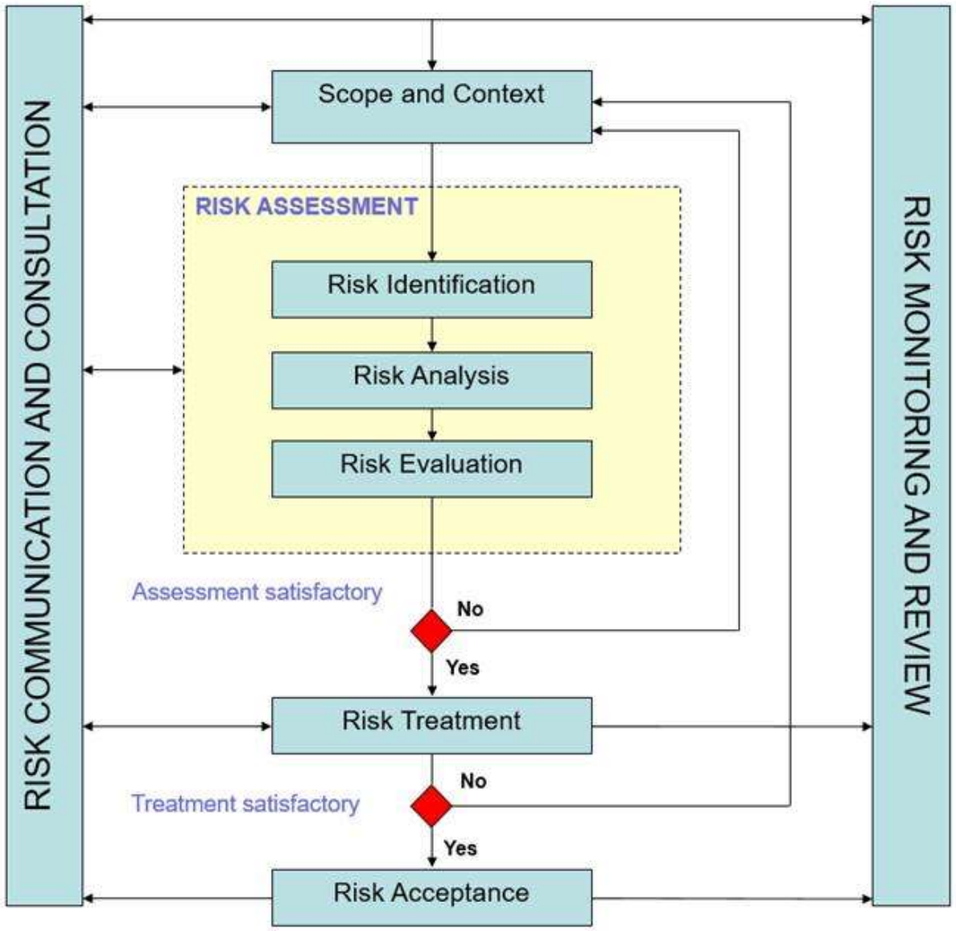
- **Preventing** an incident by **protecting** the system from an attack
- **Responding** appropriately when an attack occurs
- **Recovering** to normal operations as safely/quickly as possible



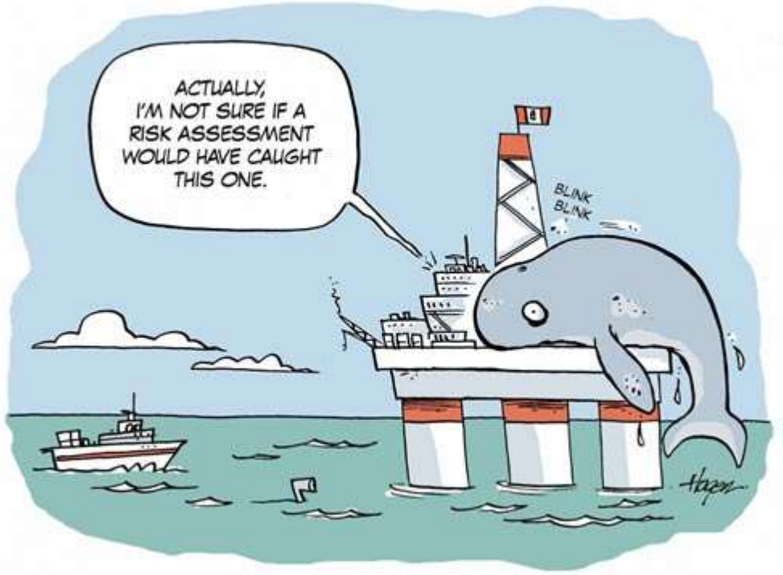
Incident Preparedness and Operational Continuity Management (IPOCM – ISO 22399)

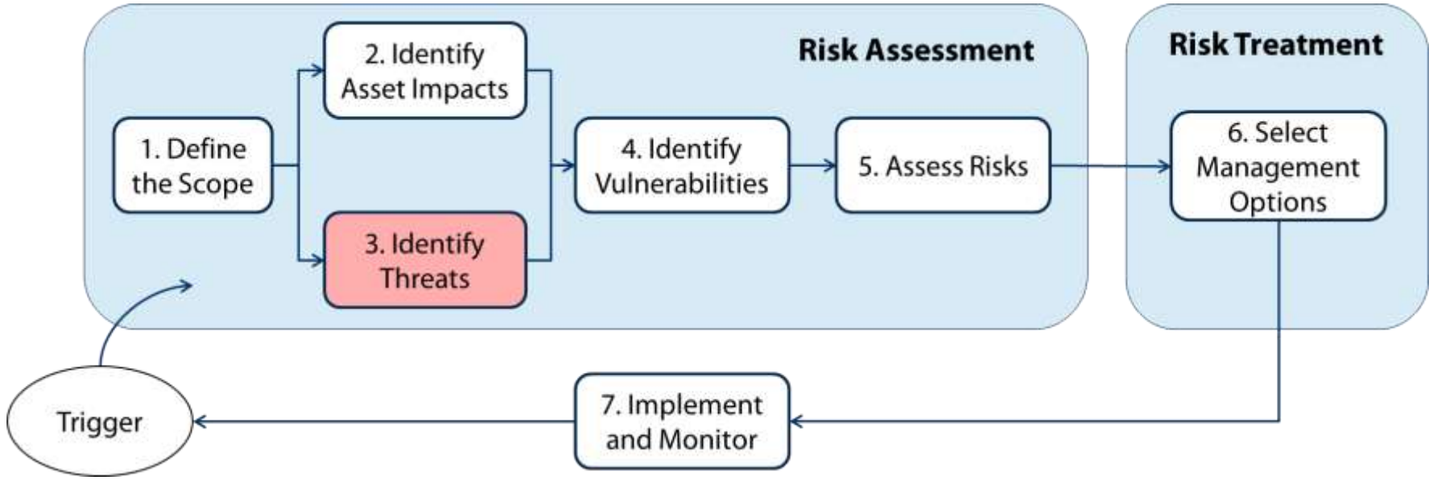
- **Resilience** is realised by
  - performing a ***Security Risk Assessment*** to identify ***what*** needs to be protected and ***how***
  - implementing a ***Security Incident Management Process*** to ensure an effective ***response***

Security Risk Assessment Methods



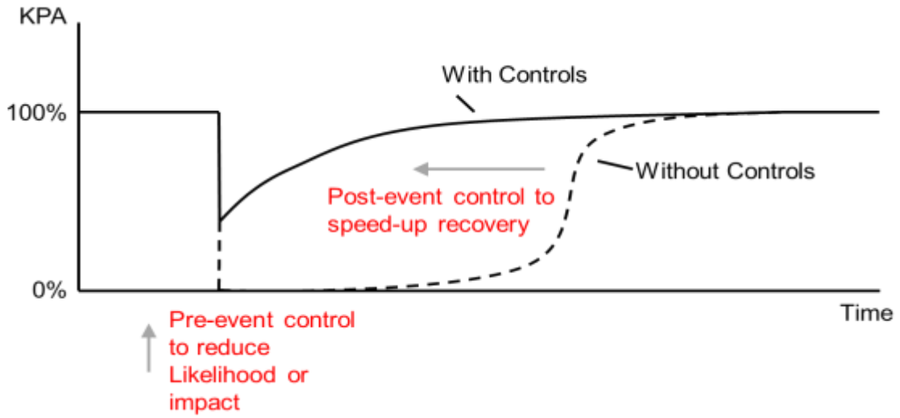
From ISO/IEC 27005

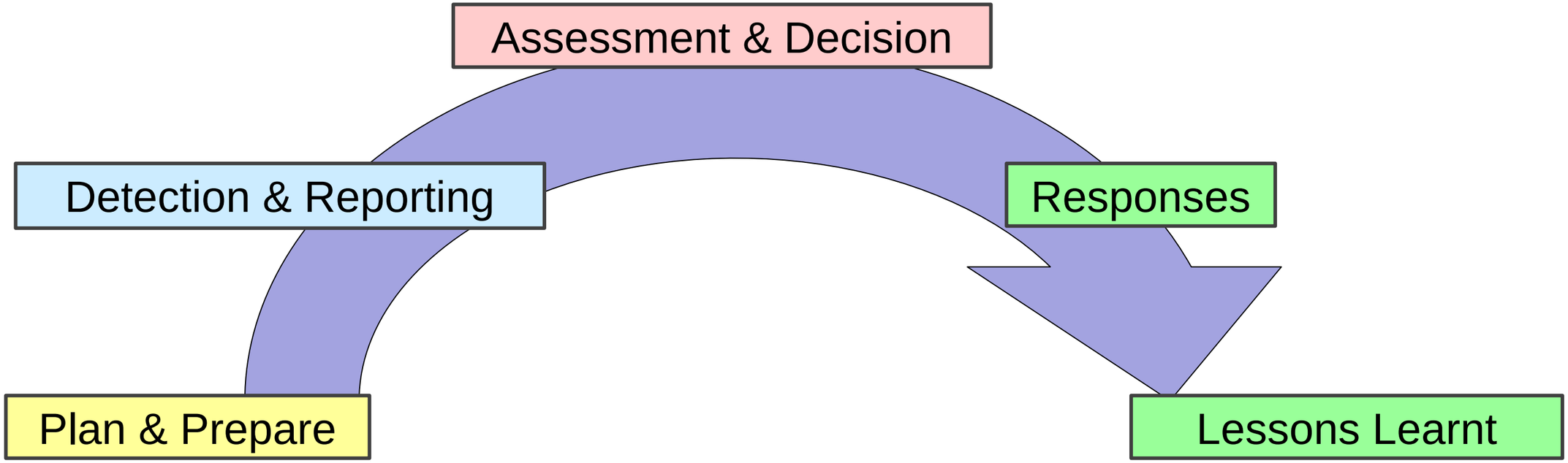




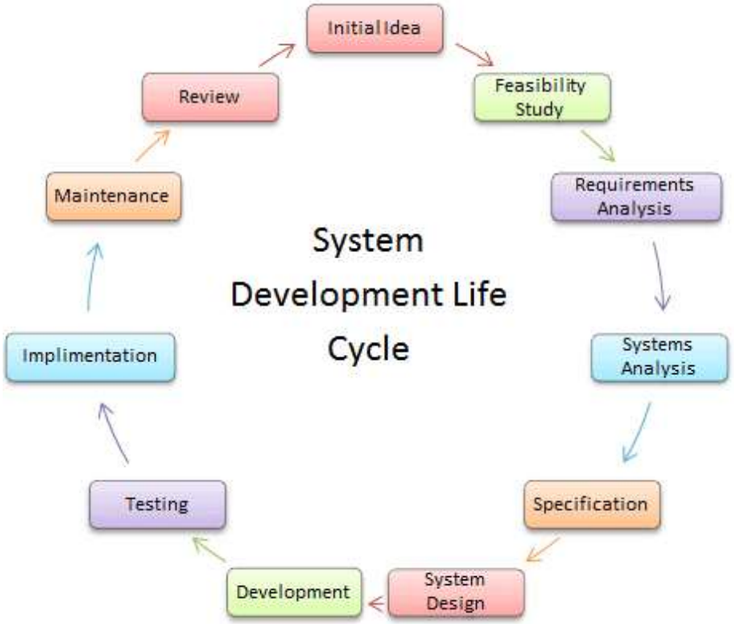
From ICAO Doc. 9985

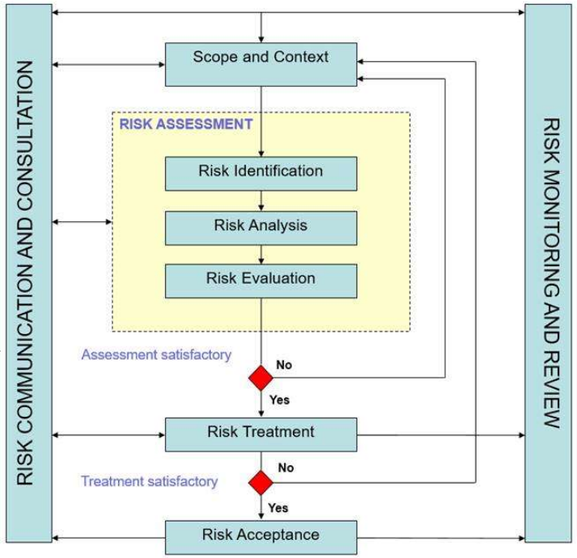
Incident Management Process (ISO/IEC 27035)



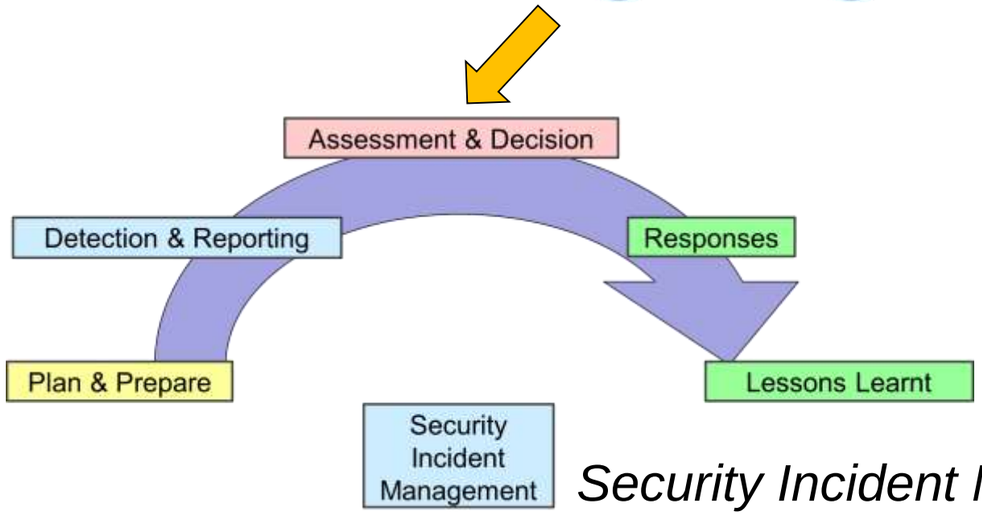


The System Life Cycle and Security Management



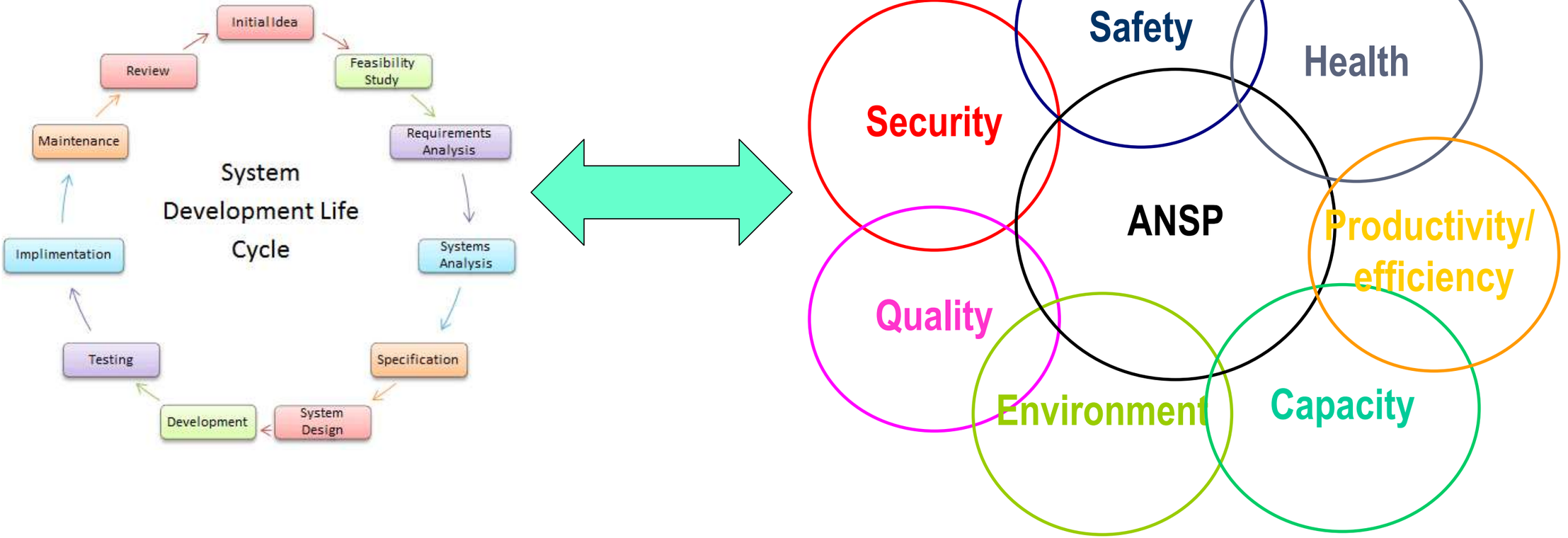


Security Risk Assessment ISO 27005



Security Incident Management ISO 27035

Transversal Areas

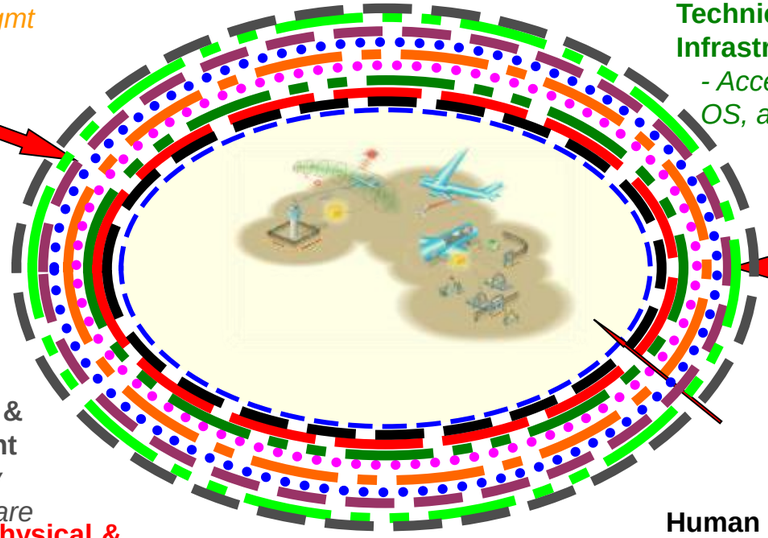


Holistic Approach to Controls

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Operation of ICT Systems
- *Systems isolated*
- *Network security*
- *Backups*
- *Change mgmt*

Organisation, Culture & Management
- *Clear roles & Responsibilities*
- *Risks managed*



Technical Mechanisms & Infrastructure
- *Access control – networks, OS, applications, user mgmt.*

Compliance
- *Legal, Policy, Standards*

Corporate Direction & Policy
- *Policy supported*

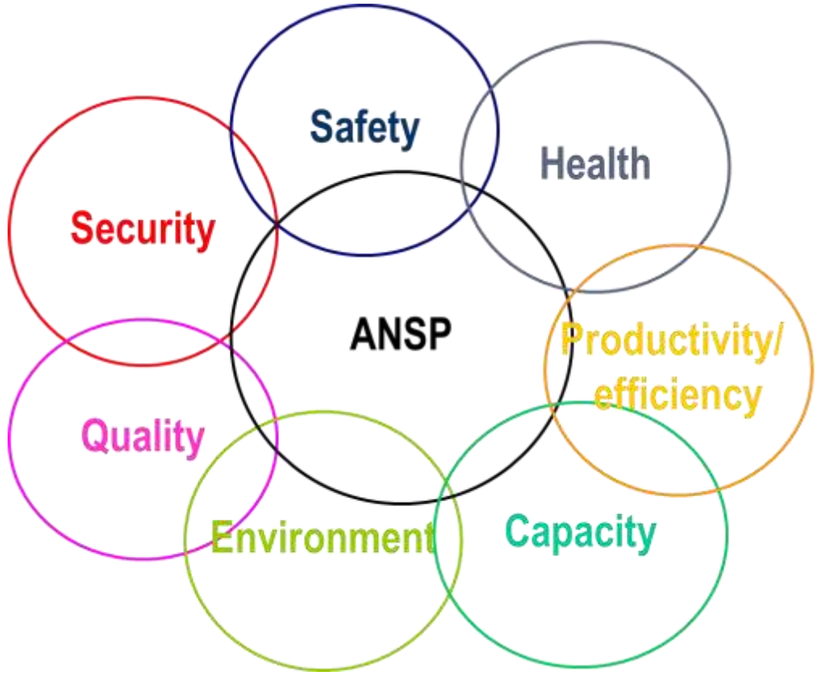
Acquisition & Development
- *IS security*
- *Anti-malware*

Monitoring & Audit
- *Logging*
- *Audits*

Physical & Environmental Security
- *Secure perimeter*
- *Equipment maintenance*
- *…*

Human Resources
- *Training*
- *Vetting*
- *…*

From ISO 27002

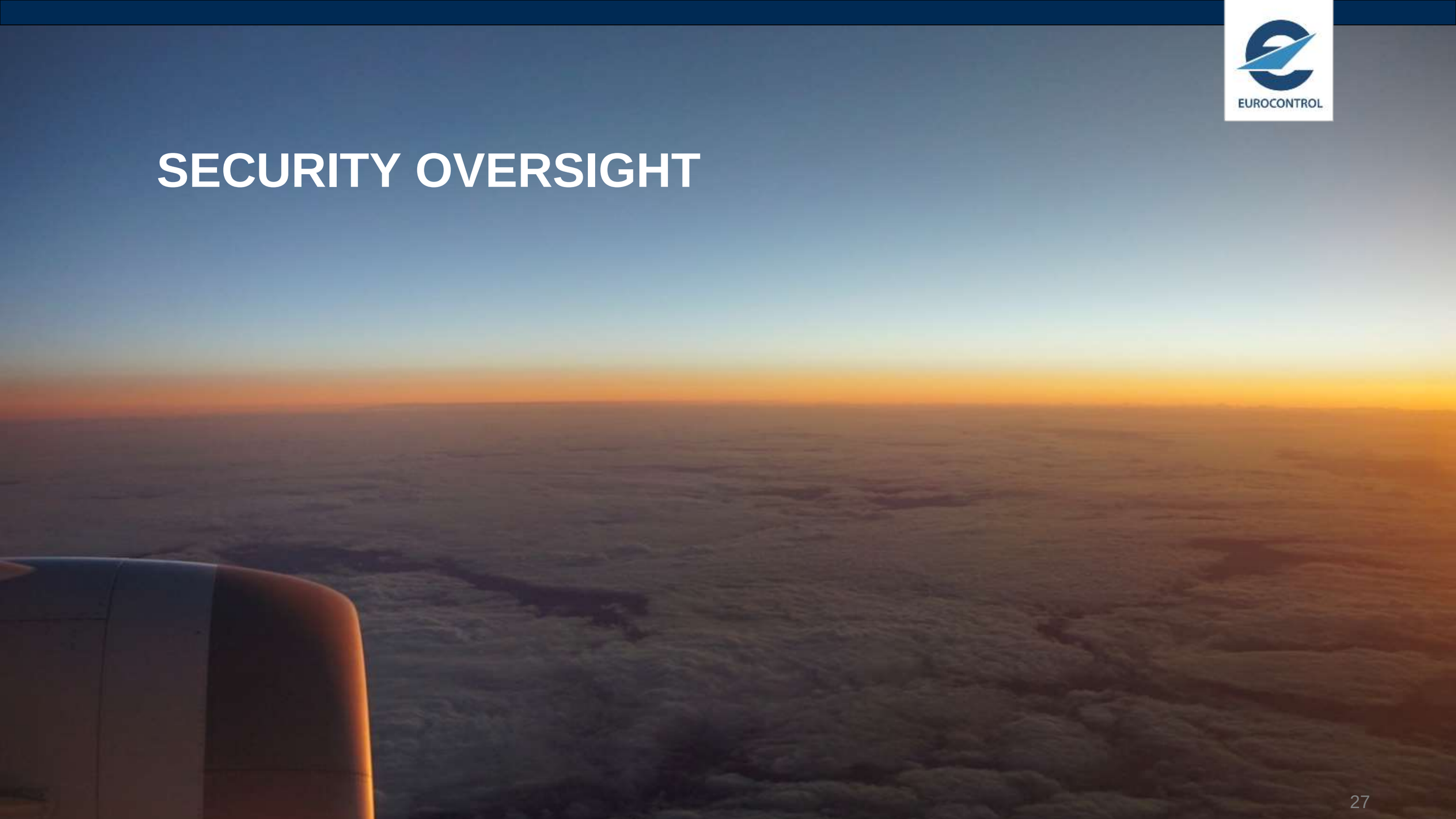


If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology. Bruce Schneier

Implementing Controls

"I think we need to take another look at your risk-management strategy."

SECURITY OVERSIGHT



Oversight Levels

GLOBAL

ICAO

States:
CAA

ANSPs

(Pan)-European

EASA

States:
NSA, CAA

FAB ANSPs
State ANSPs

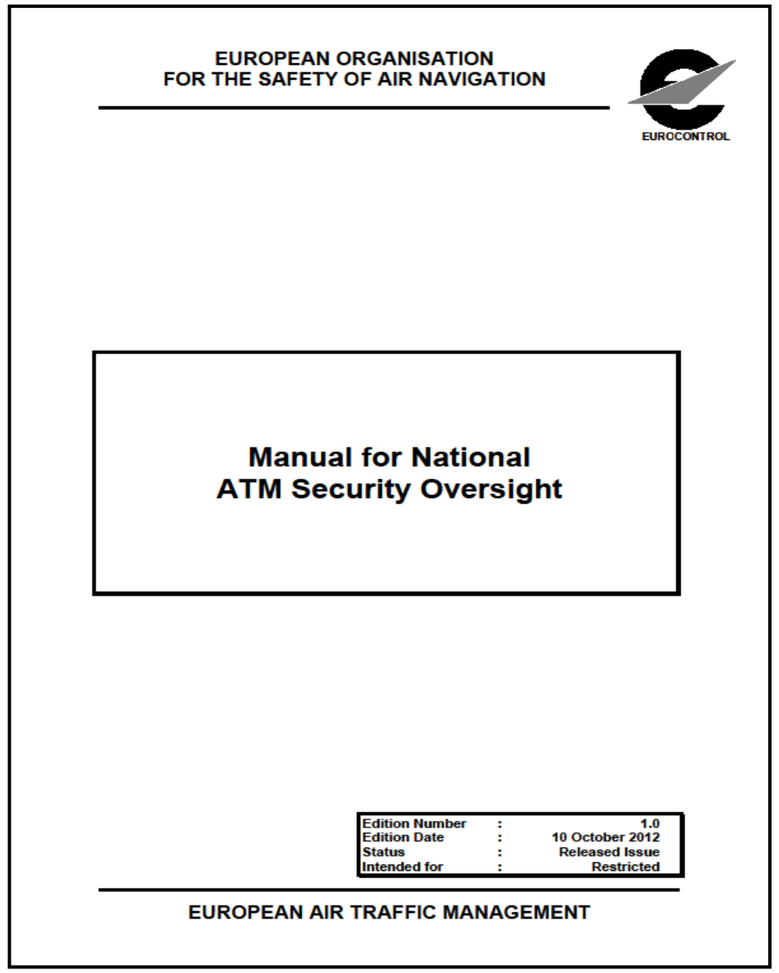
Types of Audits and Inspections

Monitoring Activity	Content	Characteristics
➢ **Security audit**	In-depth (as exhaustive as possible) examination of **all** aspects of the NCASP requirements	▪ Timing: from a number of days to one ▪ month ▪ Multi-site/location ▪ Should always be announced in advance ▪ Should not include overt or cover security tests
➢ **Security inspection**	Examination of implementation of relevant provisions in the NCASP	▪ Narrower scope than an audit ▪ Focuses on a specific activity ▪ May be announced in advance ▪ May include overt or cover security tests
➢ **Security test**	Simulation of an attempt to commit an unlawful act to test a security measure	▪ May be overt or cover security tests ▪ Only demonstrate if a security measure or control proved effective at a specific place and time ▪ Focus on access control to restricted areas, protection of assets etc.
➢ **Security survey**	Evaluation of security needs	➢ **Is intended to:** ▪ Highlight vulnerabilities that could be exploited to carry out an act of unlawful interference ▪ Recommend corrective actions ▪ Should be carried out whenever a threat necessitates an increased level of security ▪ The scope ranges from targeted assessment focused on a specific operation to an overall evaluation of security measures ▪ Timing: from a few hours to several weeks ▪ Should include overt or covert security tests

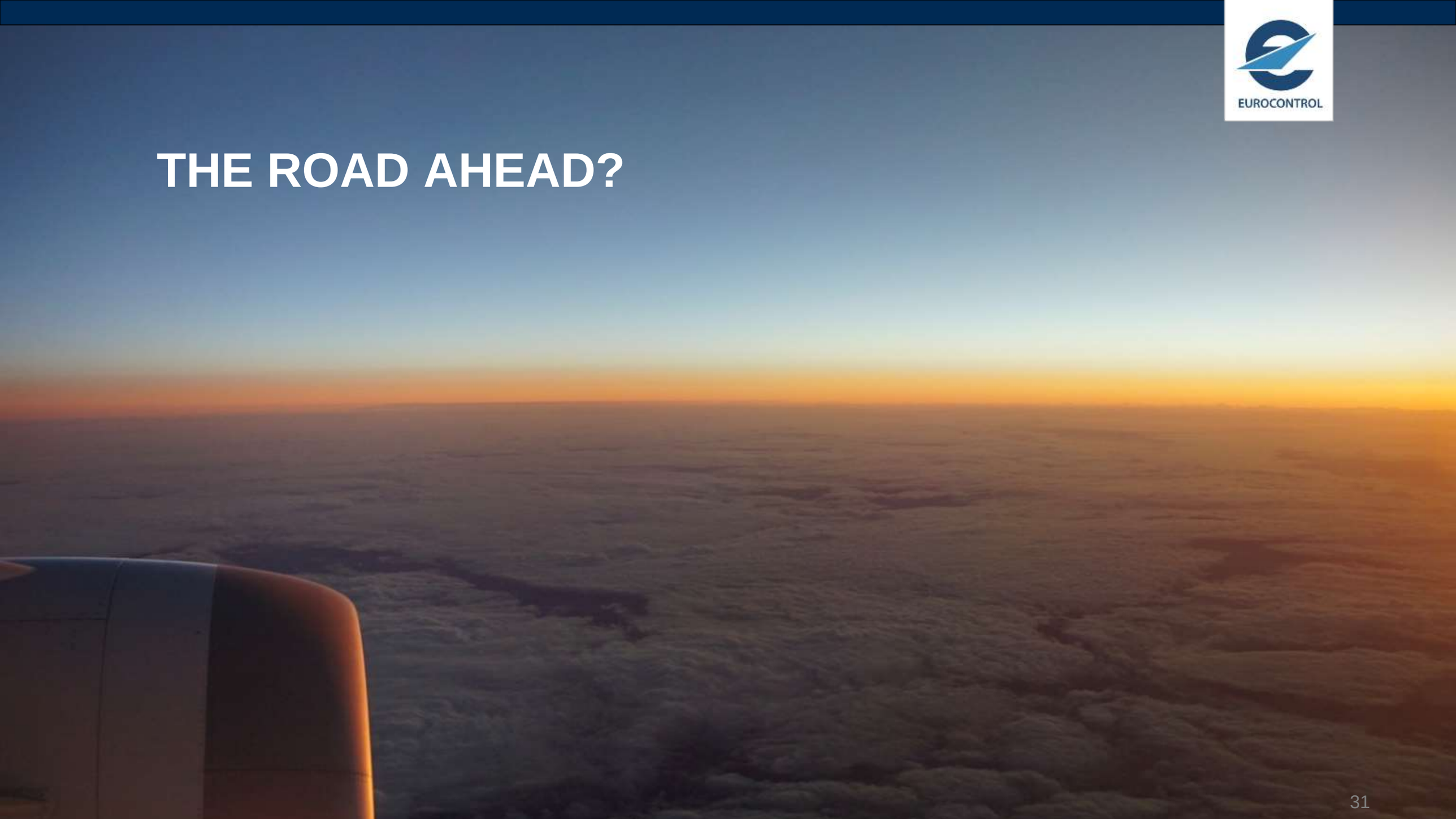
Oversight Guidance Material

Aviation Security Oversight Manual

ICAO Doc 10047



THE ROAD AHEAD?



The Stairway to Security Nirvana

A personal view

Incidents : Collaborative Response, Recovery

Incidents : Share Information

System-wide Common Minimum Security Level

Trust Framework

Share Assessment Results

Perform Risk Assessments

Tool Support

Mitigate Risks

Minimum Security Level

Security Awareness

Security Training

Security Workshops

Security Culture Development

Compatible Security Risk Assessment Approach

Compatible Standards, Guidelines

Security / Safety Interface

Vision

R&D

Security Policy

Security Management System

Security by Design

Holistic Approach

MENTI QUIZ : OVERSIGHT

- **Q9 : What kind of monitoring activity is a Test?**

EUROCONTROL ACTIVITIES AND GASEP KEY PRIORITIES

EUROCONTROL and GASeP Outcomes

Enhance Risk Awareness and Response

***NEASCOG** – NATO EUROCONTROL ATM Security Coordination Group*

- Works in support of the ICAO AVSEC/TRWG (Threat & Risk Working Group) :
  - Threat assessments on CNS cyber and non-cyber threats
  - Produces a regional assessment used in the Risk Context Statement (RCS)
  - Each State adapts the RCS to its own threat environment
  - Specific threat and risk assessments also carried out (e.g. RPAS, ADS-B, in the context of the SESAR programme)

Develop Security Culture and Human Capability

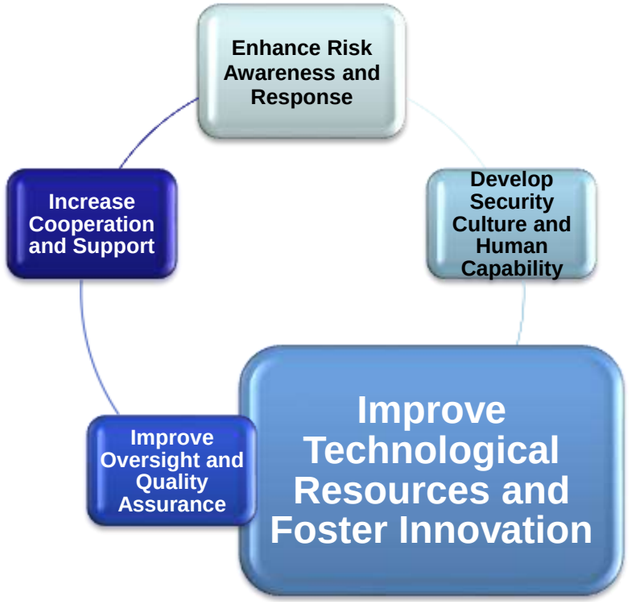
Institute for Air Navigation Services (IANS)

EUROCONTROL ATM Security Training Courses :

- Security Management Systems (3 days)
- Cyber Security (5 days)
- Security Regulatory Framework (2 days)
- Security for Operational Staff (2 days)
- Security Introduction for Senior Management (in development)
- EUROCONTROL / ICAO agreement signed under ICAO TRAINAIR Plus Corporate Partnership umbrella
  - Pilot course in development

Improve Technological Resources and Foster Innovation

European R&D Programmes



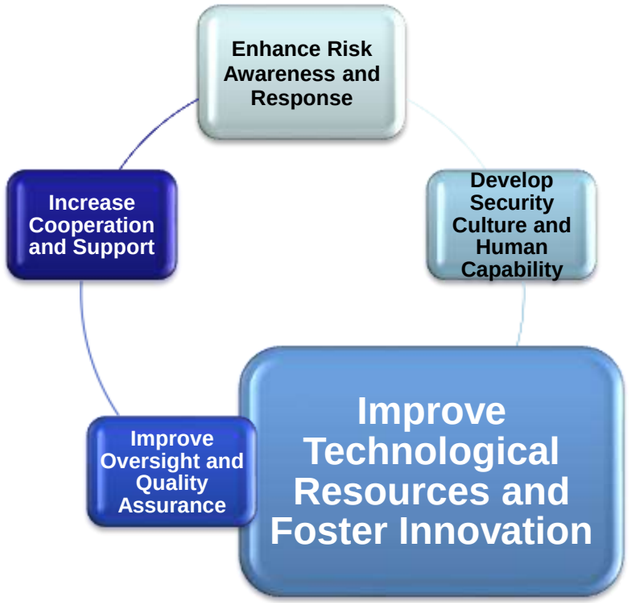
- Co-chair of WG4 on Safety and Security in ***ACARE*** programme *(Advisory Council for Aviation Research & Innovation in Europe)*
  - Maintains a road map for future R&D activities to reach goals of *Flightpath 2050*

- Participates in ***OPTICS2*** project *(Observation Platform for Technological and Institutional Consolidation of Research in Safety & Security)*
  - Assesses the progress of research to identify gaps and overlaps en-route to *Flightpath 2050* vision

Improve Technological Resources and Foster Innovation (2)

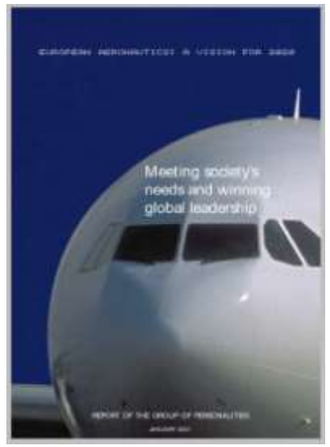
European R&D Programmes

- Founding member of ***SESAR*** Joint Undertaking *(Single European Sky ATM Research)*
  - Key participant in ***SESAR2020*** programme – maintains security risk assessment method, provides guidance on projects (PENS, SWIM, common KPI, ATM CERT, SoC for Network Manager, …)



- Advisory board member on several European Union ***Horizon2020*** projects
  - PACAS, SATIE, SeCoIIA, …

Improve Technological Resources and Foster Innovation (3)



2001 – 2020 Vision

ACARE

Anticipating future research needs

ACARE

SESAR JOINT UNDERTAKING

Integrating security into R&D, deployment

SESAR **SESAR 2020**

2011 - Flightpath 2050

optics²

Analysing current research programmes

OPTICS **OPTICS2**

Improve Oversight and Quality Assurance

Support to States Programme

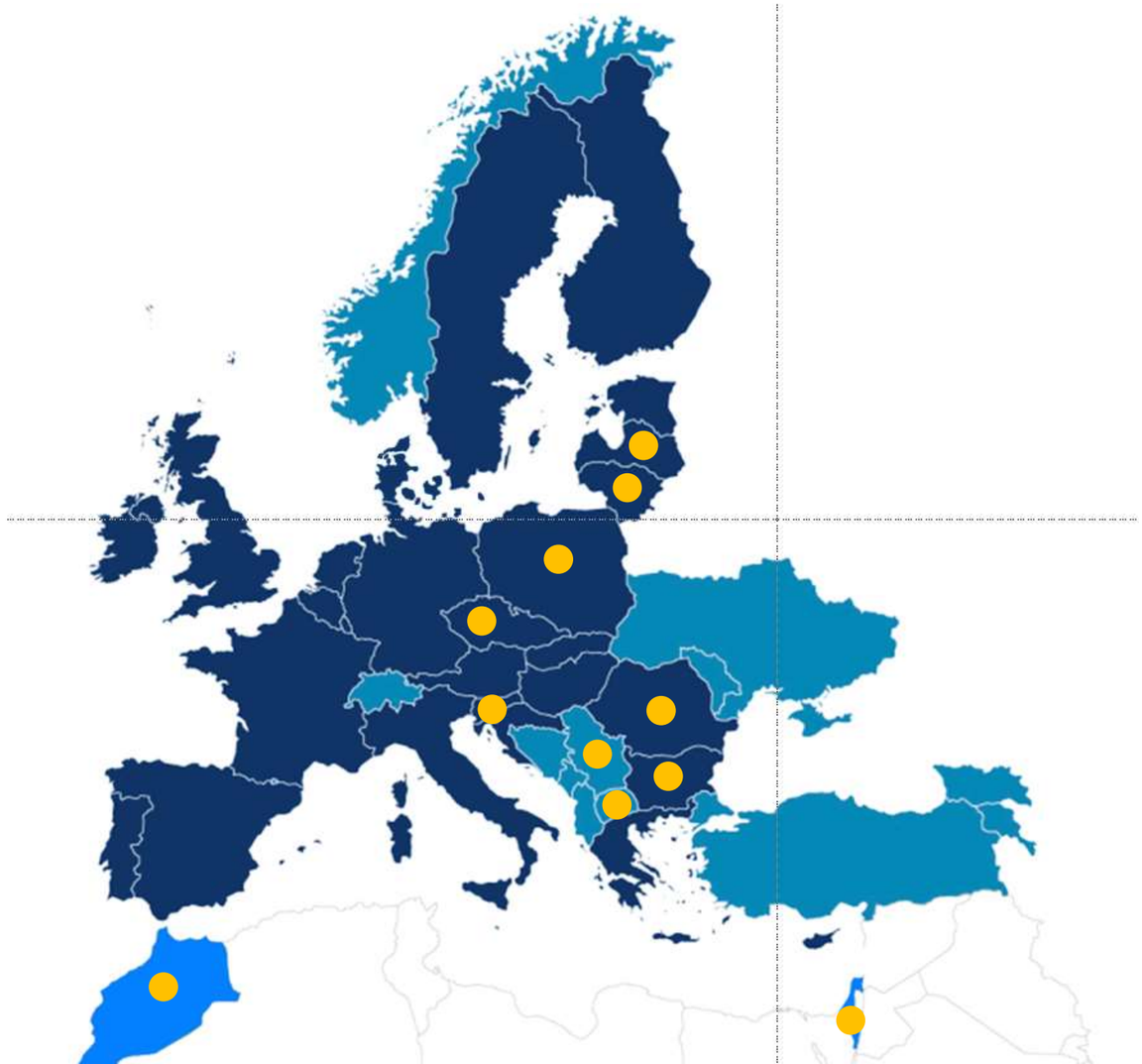
- Conduct workshops in Member States
  - Audience
    - Appropriate Authorities
    - CAAs
    - ANSPs
    - National Cyber CERT
  - National Oversight Requirements
    - Regulatory compliance (ICAO SARPS, EU Regulations)
    - “EUROCONTROL Manual for National ATM Security Oversight”
  - Cybersecurity
- Workshops tailored to needs of Member States

Improve Oversight and Quality Assurance (2)

Support to States Programme

2017-2019

- Lithunia
- Latvia
- Poland
- Czech Republic
- Slovenia
- Romania
- Bulgaria
- Serbia
- North Macedonia (FYROM)
- Morocco
- Israel
- Slovenia



Increase Cooperation and Support

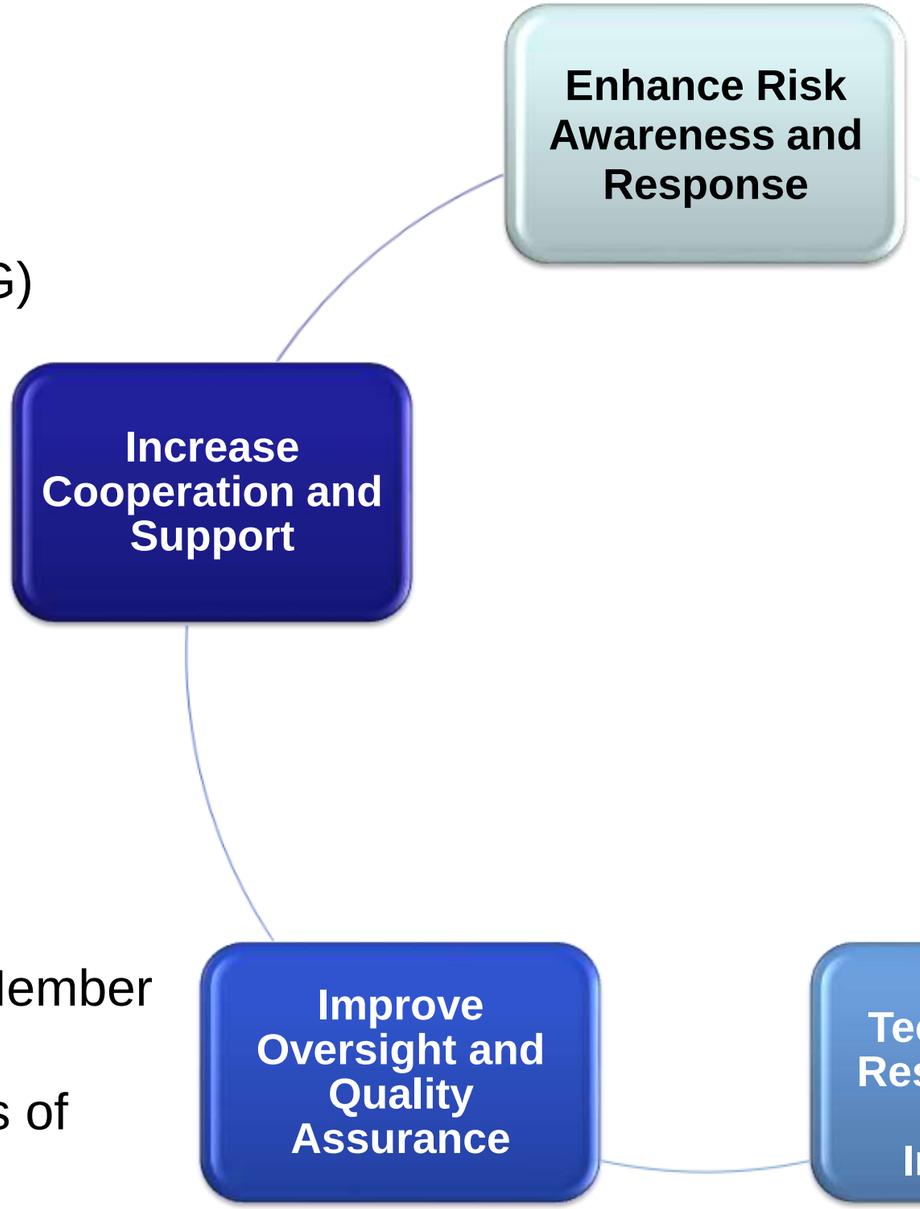
- **ICAO**
  - EUR/NAT Aviation Security Group (ENAVSEG)
  - AVSEC Threat and Risk Working Group (TRWG)
  - AVSEC Panel
  - Secretariat Study Group on Cybersecurity (SSGC)
  - INNOVA project – Aviation Trust Framework
  - TRAINAIR Plus programme
- **European Commission**
  - SAGAS – Stakeholders Advisory Group on Aviation Security (DG Move)
  - ACARE - co-chair WG4, Safety and Security)
  - OPTICS2
  - SESAR, SESAR2020
- **EASA**
  - ESCP - European Strategic Coordination Platform

Increase Cooperation and Support (2)

- **NEASCOG**
  - Common policies, strategy, guidance, awareness and training
- **ECAC**
  - Member of *ECAC Security Forum*
  - Security lead in *Guidance Material Task Force*
  - Contribute to *ECAC Study Group on Cyber Threats to Civil Aviation*
- **EDA**
  - Mapping activities and actors in aviation cyber security domain
  - NEASCOG Work Programme
  - Military buy-in to SESAR R&D, Deployment, EASA Regulations
- **EUROCAE**
  - Lead development of ED205

    "Process Specifications for Security Certification and Declaration of ATM/ANS Ground Systems"
- **EATM-CERT Services**
  - Internal, national CERTs, ANSPs, AOs

EUROCONTROL and GASeP Outcomes - Summary



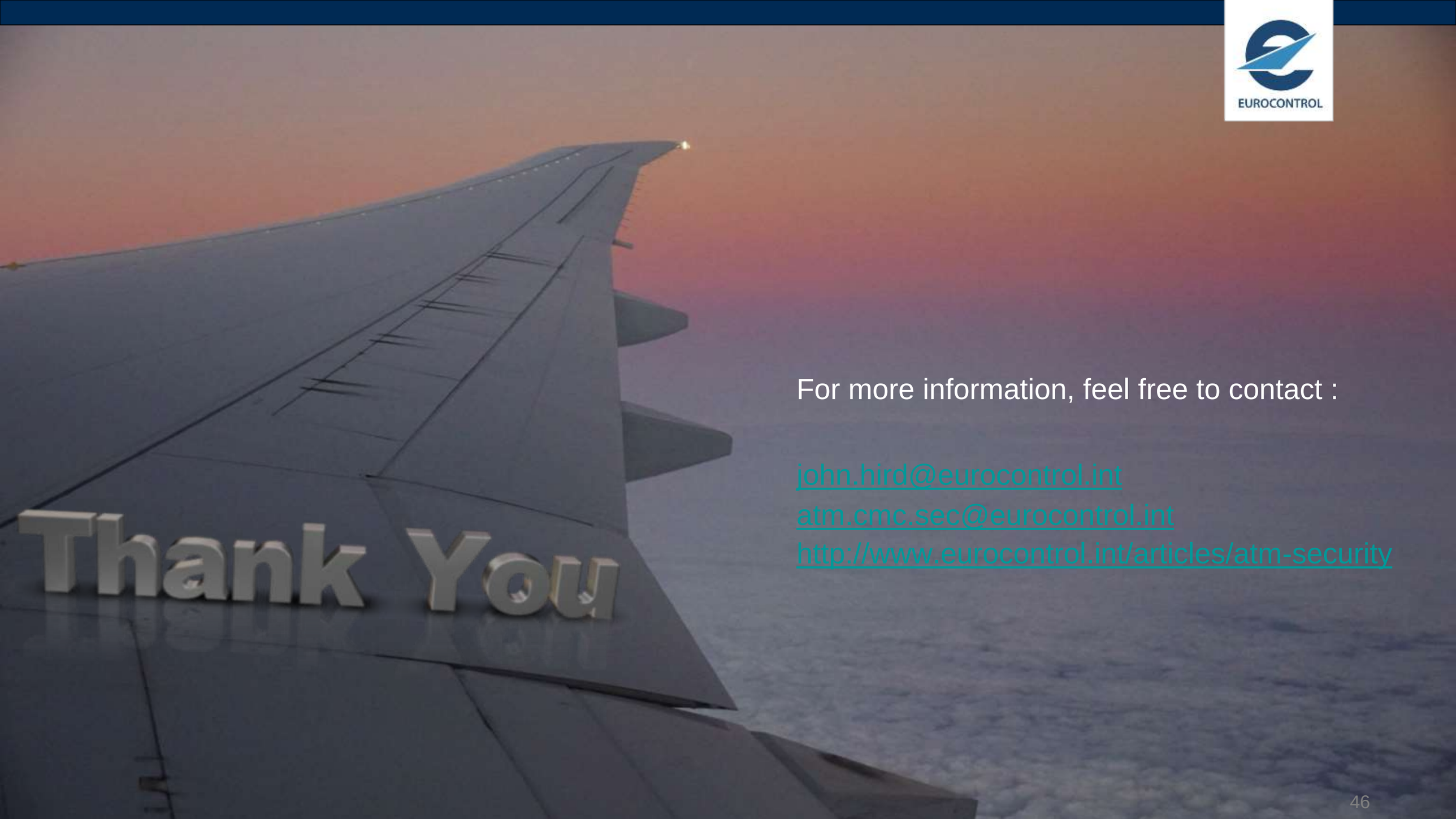
Cooperating with
- ICAO (Training)
- NATO (NEASCOG)
- ECAC
- EASA
- EDA
- EUROCAE
- Member States
- CAAs
- ANSPs
- National CERTs

NEASCOG
- ICAO AVSEC/TRWG
- RCS

Training courses
- ICAO Trainair Plus Corporate Partnership agreement
- RCS

Support to States
- Workshops for Member States
- Tailored to needs of State

European R&D Programmes
- ACARE
- OPTICS2
- SESAR2020
- Advisory boards



For more information, feel free to contact :

john.hird@eurocontrol.int
atm.cmc.sec@eurocontrol.int
http://www.eurocontrol.int/articles/atm-security

MENTI : WORKSHOP AREA KNOWLEDGE

MENTI : WORKSHOP FEEDBACK

MENTI QUIZ : ULTIMATE PATIENCE AWARDS

- **Q10 : Final Question**